Consultation on Root Zone KSK Rollover

2012-12-14

Consultation Objective

The Internet Assigned Numbers Authority (IANA) Functions contract (SA1301---12---CN---0035) between ICANN and the United States Department of Commerce, National Telecommunications Information Administration (NTIA) to perform services related to certain interdependent Internet technical management functions calls for a public consultation from all interested and affected parties to help satisfy the following objective:

> **C.2.9.2.f Root Domain Name System Security Extensions (DNSSEC) Key Management** –The Contractor shall be responsible for the management of the root zone Key Signing Key (KSK), including generation, publication, and use for signing the Root Keyset. As delineated in the Requirements at Appendix 2 entitled Baseline Requirements for DNSSEC in the Authoritative Root Zone that is incorporated by reference herein as if fully set forth. The Contractor shall work collaboratively with NTIA and the Root Zone Maintainer, in the performance of this function.[1]

More specifically, this consultation involves "**Appendix 2: Baseline Requirements for DNSSEC in the Authoritative Root Zone,"** that articulates the contract requirement to perform a scheduled root zone KSK rollover.[2]

The consultation is being conducted using the ICANN Public Comment Process, consistent with the contract requirements. The feedback received during this consultation will inform the Root Zone Management Partners on the subject of KSK rollover, so that a schedule and a detailed implementation plan for KSK rollovers can be established.

This Consultation

This consultation requests input from the community regarding the scheduling and implementation of future KSK rollovers.

Background and Context

The following subsections are intended to provide background and context for commenters in considering the issue of scheduling and implementing root KSK rollovers. More extensive documentation on the processes and systems involved in the

---

[1] See page 8 of the IANA functions contract, section C.2.9.2.f, http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

[2] See page 20 of the IANA functions contract, Appendix 2, section c) Root Zone KSK Rollover, http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

use of DNSSEC in the root zone has been published[3] and may provide further useful insight.

DNSSEC Deployment in the Root Zone and KSK Generation

ICANN, Verisign and NTIA (the Root Zone Management Partners) concluded a successful collaboration to deploy DNSSEC in the root zone of the DNS in July 2010. ICANN and Verisign each published details of how their respective duties are performed in the documents "DNSSEC Practice Statement for the Root Zone KSK Operator"[4] and "DNSSEC Practice Statement for the Root Zone ZSK Operator"[5], respectively.

The active KSK was generated during KSK Ceremony 1 on 2010-06-17 at KMF-East[6]. Secure transport of the key materials to KMF-West[7] concluded during KSK Ceremony 2, following which the KSK was designated to be in full production. All subsequent KSK Ceremonies have made use of that same KSK.

Scheduled KSK Rollover

No KSK rollover has been executed since the active KSK was designated to be in full production. However, the IANA Functions Contract specifies a high-level requirement to perform KSK rollover in the root zone "as required or after five years."

The IANA Functions Contract[8] specifies:

> 1.2.9.2.f.3.9.3 Root Zone KSK Rollover
>
> Root Zone KSK rollover will be executed as required or after five years of operation. Cryptographic algorithm rollover will also be taken into account when planning a [Root Zone] KSK rollover.
>
> The [Root Zone] KSK rollover will be scheduled to facilitate automatic updates of the Trust Anchors in the DNS resolvers as described in RFC 5011. This rollover will allow seamless transition from the old Trust Anchor to the new Trust Anchor without jeopardising the chain of trust. After a [Root Zone] KSK has been removed from the key set, it will be retained after its operational period until the next scheduled key ceremony, which is when the private component will be destroyed in a secure manner.

At the time that the active KSK was generated, software available to perform DNSSEC validation was considered relatively immature. Therefore, detailed scheduling of KSK

---

[3] http://www.root-dnssec.org/
[4] https://www.iana.org/dnssec/icann-dps.txt
[5] http://www.verisigninc.com/assets/dnssec-practice-statement-root-zone-zsk-operator.pdf
[6] Key Management Facility (KMF)-East is located in Culpeper, VA, USA.
[7] KMF-West is located in El Segundo, CA, USA.
[8] http://www.ntia.doc.gov/page/iana-functions-purchase-order

rollover was deferred until the reaction of such software to a KSK rollover was better understood.

Existing KSK Management Software

The software used during KSK Ceremonies is capable of generating a new key and of managing a KSK rollover.

The ability of the software and related processes to generate a new KSK and transport it securely between KMFs was demonstrated during KSK Ceremonies 1 and 2.

The KSK rollover capability of the software was tested during public, pre-production testing and an independent report published prior to full production confirmed that all key transitions were observed to follow RFC 5011 semantics.

Impact on Human Resources

The impact on human resources (and other associated costs) is an important consideration for the scheduling and implementation of KSK rollovers.

Currently, KSK Ceremonies are scheduled four times per year, and involve both ICANN staff and TCRs. TCRs are volunteers chosen from all ICANN regions who travel without funding from ICANN.

It is important to note that a KSK rollover would require specific actions to be taken at a KSK Ceremony and has the potential (depending on schedule and frequency) to significantly impact the human resources involved and other associated costs, such as travel for the TCRs who need to participate in the KSK Ceremonies.

An aggressive KSK rollover schedule that required more frequent KSK Ceremonies to be scheduled would increase the time and travel commitment for those involved in KSK Ceremonies.

Operational Lifetime of Hardware Security Modules (HSMs)

It is important to note that the lifetime of HSMs has implications for the KSK and should be considered with respect to a KSK rollover schedule and implementation.

Existing processes for KSK rollover involve the generation of an incoming KSK on a newly-accepted HSM. The HSM containing the outgoing KSK is retained until the operational period of the outgoing KSK has passed, and is subsequently destroyed in a secure manner.

The effective operational lifetime of the HSMs in use is determined by the lifetime of the HSMs internal batteries. The vendor of the HSMs in use guarantees the batteries for five years of operation. There are therefore some efficiencies in adopting a KSK rollover schedule with a period less than or equal to five years, since the HSM replacement required for the KSK rollover can coincide with the HSM replacement that would otherwise be needed to ensure battery life.

Publication of the Root Zone Trust Anchor

The set of current DNSSEC trust anchors for the root zone are published[9] in a way that accommodates the retirement of an active KSK and the promotion of a newly-published KSK to active. Retired trust anchors will continue to be published, but will be specified as having a validity period in the past.

There is no change to the publication of DNSSEC trust anchors for the root zone required to accommodate a KSK rollover.

Consultation Questions

ICANN, consistent with the terms of the IANA functions contract, is committed to executing a KSK rollover in the root zone and now seeks public feedback with respect to developing a detailed scheduling and implementation plan.

Comments are welcome on any aspect of KSK management related to KSK rollover, and specifically on the following questions:

1. What prerequisites need to be considered prior to a first scheduled KSK rollover?
2. When should the first scheduled KSK rollover take place?
3. What should the IANA Functions Operator (ICANN) and the other Root Zone Management Partners do to gauge the technical and end-user impact of a KSK rollover following the first scheduled KSK rollover?
4. How often should a scheduled KSK rollover take place, following the first one?
5. How far should the published calendar for scheduled KSK rollovers extend into the future?
6. What public notification should take place in advance of a scheduled KSK rollover?
7. What other considerations are necessary for the Root Zone Management Partners to take into consideration prior, during, and after a planned key roll over?

[9] J. Abley, J. Schlyter, "DNSSEC Trust Anchor Publication for the Root Zone", May 7, 2010, http://www.root-dnssec.org/wp-content/uploads/2010/07/draft-icann-dnssec-trust-anchor-01.txt

Glossary

This document makes frequent use of specialised terminology. Such specialised terms are listed here rather than being expanded at first use, in the interests of making the document easier to read by a technical audience.

Term	Meaning in This Document
DNS	Domain Name System, as originally specified in RFC 1034.
DNSSEC	DNS Security Extensions, as specified in RFC 4033.
DNSSEC Validation	The cryptographic verification of DNSSEC signatures attached to RRSets, by which the authenticity of DNS responses can be determined.
DPS	DNSSEC Policy and Practice Statement, a public document describing how DNSSEC is implemented and maintained. For the root zone, Verisign and ICANN each publish a DPS which documents their respective responsibilities.
IANA functions	A set of technical functions specified in the IANA Functions Contract administered by NTIA and currently awarded to ICANN.
ICANN	Internet Corporation for Assigned Names and Numbers, the current IANA Functions Operator.
IETF	Internet Engineering Task Force, the standards body responsible for Internet-related protocols.
KMF	Key Management Facility, the secure facility where the KSK is stored and exercised during KSK Ceremonies. The two active KMFs are located in Culpeper, VA, USA ("KMF-East") and El Segundo, CA, USA ("KMF-West").
KSK	The Root Zone Key Signing Key, a DNSSEC key-pair. The private component of the KSK is used to generate signatures over the DNSKEY RRSet; the public component provides a means to validate signatures made with the private component. Validators test the integrity of the observed public component of the KSK using a pre-configured trust anchor.
KSK Ceremony	A set of procedures carried out under secure conditions by which the KSK is generated and exercised. Ceremonies are scheduled to take place for times each calendar year.
KSK Rollover	The replacement of an active KSK with a successor. Following the KSK Rollover procedure, the previously-active KSK is retired and plays no further role.
NTIA	National Telecommunications and Information Administration.
RFC	Request for Comments, the name of a document series produced and maintained by the IETF.
Root Zone	An infrastructural zone in the DNS namespace which facilitates referrals from root servers to DNS servers that are authoritative for TLDs.
RRSet	A set of one or more DNS resource records published in a zone.
TCR	Trusted Community Representative, non-affiliated representatives of the global technical community who assist ICANN in managing the KSK during KSK Ceremonies.
TLD	Top-Level Domain, the right-most label in a domain name.
Trust Anchor	A hash (digest) of the public component of the KSK, used by validators to verify the integrity of the observed public component of the KSK.
Validator	An iterative resolver that performs DNSSEC validation.

Verisign	The party currently carrying out the role of Root Zone Maintainer under a cooperative agreement administered by NTIA.